FastIron ICX™ 7750, ICX 7250 and ICX 7150 Series Switch/Router

FIPS 140-2 Non-Proprietary Security Policy Level 1

Document Version 2.2

August 30, 2018

Contents

1 Introduction

The FastIron ICX™ 7150 family of stackable switches delivers the performance, flexibility, and scalability required for enterprise access deployment, raising the bar with non-blocking performance and up to 8x10 GbE ports for uplinks or stacking. It offers seamless interoperability with Ruckus wireless products to deliver unified wired and wireless network access. In addition, Ruckus Multigigabit Ethernet technology offers bandwidth speeds needed to optimize performance of the latest generation high performance wireless access points and edge devices, over standard Ethernet cables. This platform combines enterprise-class switching features with high performance at an entry-level price.

The FastIron ICX™ 7250 Switch delivers the performance, flexibility, and scalability required for enterprise Gigabit Ethernet (GbE) access deployment. It raises the bar with up to 8×10 GbE ports for uplinks or stacking and market-leading stacking density with up to 12 switches (576×1 GbE) per stack. In addition, the ICX™ 7250 combines enterprise-class features, manageability, performance, and reliability with the flexibility, cost-effectiveness, and “pay as you grow” scalability of a stackable solution.

The FastIron ICX™ 7750 is a 10/40 GbE Ethernet switch delivering a chassis experience for campus LAN aggregation and core. It offers unprecedented port density and chassis-level performance, availability, and scalability. The ICX™ 7750 distributed chassis technology enables scale-out networking and its true hybrid-port mode OpenFlow provides a migration path to SDN.

2 Overview

The FIPS 140-2 validation includes hardware devices running the firmware version presented in Table 1. The module meets an overall FIPS 140-2 compliance of Security Level 1 with Design Assurance Level 1.

Table 4 and Table 7 list the devices included in this evaluation.

The ICX™ 7150 devices are referred collectively for the remainder of this document as ICX 7150 device (cryptographic module, or simply the module). The ICX 7150 is available in 12, 24 and 48 port 10/100/1000 Mbps models with 1/10 GbE dual-purpose uplink/stacking ports, and full PoE/PoE+ support. The ICX 7150-48ZP offers 16 Multigigabit ports, each with PoH up to 90 watts, plus 32 10/100/1000 Mbps ports with PoE+. The ICX 7150-C12P compact 12-port stackable switch features a fanless design to operate silently in out-of-closet environments such as offices, classrooms, and retail spaces. It offers PoE+ on all 12 ports to drive devices such as wireless APs, VoIP phones, lighting fixtures or surveillance cameras. The cryptographic boundary for each ICX 7150 device is represented by the opaque enclosure (including the power supply, fan tray and bezels).

Table 4 lists the two (2) ICX™ 7250 series devices, referred collectively for the remainder of this document as ICX 7250 device (cryptographic module, or simply the module). Each ICX 7250 device is a fixed-port switch. This environment is a multi-chip standalone cryptographic module. ICX 7250 is available in PoE and non-PoE configuration. The cryptographic boundary for each ICX 7250 device is represented by the opaque enclosure (including the power supply, fan tray and bezels).

Table 7 lists the three (3) ICX™ 7750 series devices, referred collectively for the remainder of this document as ICX 7750 device (cryptographic module, or simply the module). Each ICX 7750 device is a fixed-port switch, which is a multi-chip standalone cryptographic module. The installed fans either use a push or pull configuration to move the air between the back and front of the device. Each model is orderable with either fan trays or power supply side intake (-I) or power supply side exhaust (-E) airflow. The power supplies and fan tray assemblies are part of the cryptographic boundary and can be replaced in the field. Unpopulated power supplies and fan trays are covered by opaque bezels, which are part of the cryptographic boundary when the secondary redundant power supplies and/or fans trays are not used. The cryptographic boundary for each ICX 7750 device is represented by the opaque enclosure (including the power supply, fan tray and bezels) with removable cover

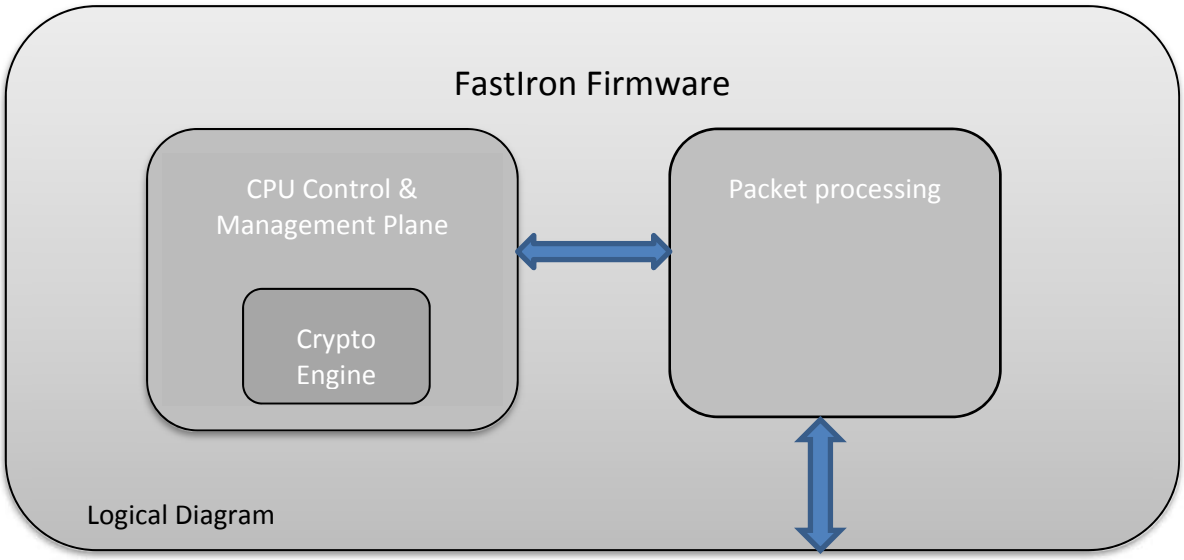

Figure 1 – Logical Diagram

3 FastIron Firmware

Each of the ICX series runs a different firmware image which is built from the same source code. This firmware image includes the cryptographic functionality described under Section 8. The firmware can be built as an “S” (switch) or an “R” (router) version. The “R” image has Router functionality in addition to the functionality in the “S” image. The source code for cryptographic module on both images is identical and is compiled identically. The “-I” and “-E” designations in Table 3 define the airflow direction as either intake or exhaust. The “-24” and “-48” designations in Table 2 define the port count, and the designator “P” following the port count indicate PoE+ ports; the designator “F” indicate Small Form-Factor Pluggable (SFP) ports. Otherwise, devices with similar SKUs are identical.

Firmware Version
IronWare R08.0.70

Table 1 - Firmware Version

4 ICX 7150 Series

Table 2 - ICX 7150 Validated Cryptographic Modules

SKU	Brief Description
ICX7150-C12P-2X10GR-A	ICX 7150 Compact Switch, twelve (12) 10/100/1000 PoE+ ports, two (2) 1G RJ45 uplink-ports, two (2) 1/10G SFP, 124W PoE budget, L3 features (OSPF, VRRP, PIM, PBR), TAA
ICX7150-24-4X10GR-A	ICX 7150 Switch, twenty-four (24) 10/100/1000 ports, two (2) 1G RJ45 uplink-ports, four (4) 10G SFP+ uplink-ports, L3 features (OSPF, VRRP, PIM, PBR), TAA
ICX7150-24P-4X10GR-A	ICX 7150 Switch, twenty-four (24) 10/100/1000 PoE+ ports, two (2) 1G RJ45 uplink-ports, four (4) 1/10G SFP+ uplink-ports, 370W PoE budget, L3 features (OSPF, VRRP, PIM, PBR), TAA
ICX7150-48-4X10GR-A	ICX 7150 Switch, forty-eight (48) 10/100/1000 ports, two (2) 1G RJ45 uplink ports, four (4) 1/10 G SFP+ uplink ports, L3 features (OSPF, VRRP, PIM, PBR), TAA
ICX7150-48P-4X10GR-A	ICX 7150 Switch, forty-eight (48) 10/100/1000 PoE+ ports, two (2) 1G RJ45 uplink-ports, four (4) 1/10G SFP+ uplink-ports, 370W PoE budget, L3 features (OSPF, VRRP, PIM, PBR), TAA
ICX7150-48PF-4X10GR-A	ICX 7150 Switch, forty-eight (48) 10/100/1000 PoE+ ports, two (2) 1G RJ45 uplink-ports, four (4) 1/10G SFP+ uplink-ports, 740W PoE budget, L3 features (OSPF, VRRP, PIM, PBR), TAA Note: (Higher power wattage than ICX715048P model)
ICX7150-48ZP-8X10GR2-A	ICX 7150 Switch, sixteen (16) 100/1000/2.5G PoH ports, thirty-two (32) 10/100/1000 PoE+ ports, eight (8) 1/10G SFP+, L3 features (OSPF, VRRP, PIM and PBR). Two (2) RPS17 Power Supplies, two (2) Fan trays. TAA

Table 3 – ICX 7150 Optional Component Part Numbers

SKU	Brief Description	Notes
RPS20	Power supply FRU for ICX7150-48ZP	See note 1
ICX-FAN11	Fan FRU for ICX7150-48ZP	See note 2

Notes:

1. RPS20 power supply is used for ICX7150-48ZP model. These power supplies are already included in the bundled SKU for ICX7150-48ZP. It is being mentioned here for sake of completeness and the fact that it is a FRU component part of the device.
2. ICX-FAN11 are used for ICX7150-48ZP and are already included as part of the bundled SKU for ICX7150-48ZP.

ICX 7150 images

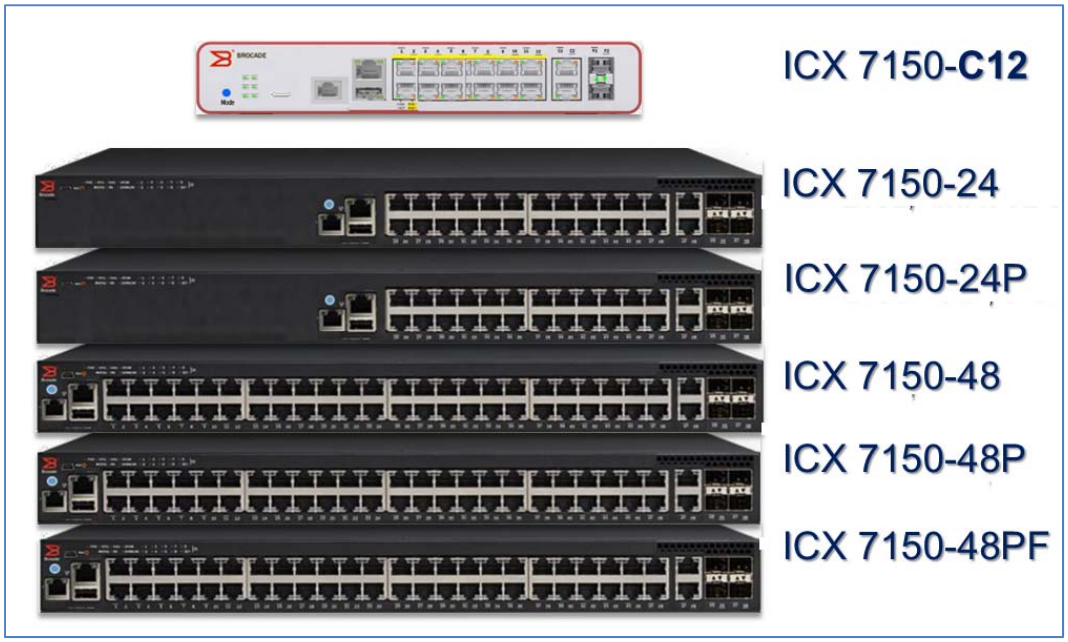

Figure 2 - Front view Images of ICX 7150 cryptographic modules

Figure 3 - Rear view Images of ICX 7150 cryptographic modules

5 ICX 7250 Series

Each ICX7250 device validated within this implementation includes the following:

SKU	MFG Part Number	Brief Description
ICX7250-24G	80-1008379-02	24 Ports 4X1G SFP
ICX7250-48P	80-1008386-02	48 Ports POE+ 8X1G SFP+

Table 4 - ICX7250 Switch Family Part Numbers of Validated Cryptographic Modules

SKU	Brief Description	Notes
EPS4000	External Power supply Shelf (4 power supply bays with 8 connectors)	See note 1
RPS17	Power supply FRU for ICX7150-48ZP or EPS4000 Power Shelf (920W)	See note 2

Table 5 – ICX 7250 Optional Component Part Numbers

Notes:

1. EPS4000 is one of the methods for supplying powering to the ICX 7250. This unit does not perform any cryptographic function.
2. RPS17 power supply is used for EPS4000. It is being mentioned here for sake of completeness.

Figure 4 through Figure 9 illustrates an ICX7250-24G cryptographic module:

Figure 4 - Front/top side of the module ICX7250-24G

Figure 5 - Back side of the module ICX7250-24G

Figure 6 - Right side of the module ICX7250-24G

Figure 7 - Left side of the module ICX7250-24G

Figure 8 - Top side of the module ICX7250-24G

Figure 9 - Bottom side of the module ICX7250-24G

Figure 10 through Figure 15 illustrate an ICX7250-48P cryptographic module:

Figure 10 - Front/top side of the module ICX7250-48P

Figure 11 - Back side of the module ICX7250-48P

Figure 12 - Right side of the module ICX7250-48P

Figure 13 - Left side of the module ICX7250-48P

Figure 14 - Top side of the module ICX7250-48P

Figure 15 - Bottom side of the module ICX7250-48P

6 ICX 7750 Series

Each ICX 7750 Series device validated within this implementation includes the following ICX modules:

SKU	MFG Part Number	Brief Description
RPS9I	80-1007871-01	500 W AC power supply; power-supply-side intake (port-side exhaust) airflow
RPS9E	80-1007870-01	500 W AC power supply; power-supply-side exhaust (port-side intake) airflow
RPS9DCI	80-1007872-01	500 W DC power supply; power-supply-side intake (port-side exhaust) airflow
RPS9DCE	80-1007873-01	500 W DC power supply; power-supply-side exhaust (port-side intake) airflow
ICX7750-FAN-I	80-1007738-01	Fan kit of 4 fans; fan-side intake (port-side exhaust) airflow
ICX7750-FAN-E	80-1007737-01	Fan kit of 4 fans; fan-side exhaust (port-side intake) airflow
ICX7750-FAN-I- SINGLE	80-1007761-01	Fan single unit; fan-side intake (port-side exhaust) airflow
ICX7750-FAN-E- SINGLE	80-1007760-01	Fan single unit; fan-side exhaust (port-side intake) airflow
ICX7750-6Q	80-1007632-01	ICX 7750 with 6 40 GbE QSFP module for use in ICX 7750- 48F, 7750-48C, or 7750-26Q

Table 6 - Components of the ICX 7750 Series

Configuration	SKU	MFG Part Number	Quantity	Brief Description
IC7750 Config 1	ICX7750-48F	80-1007607-01	1	ICX 7750 with 48 1/10 GbE SFP+ ports, 6 40 GbE QSFP ports and modular interface slot. No power supplies or fan units (need to be ordered separately).
	RPS9E	80-1007870-01	2	500 W AC power supply; power-supply-side exhaust (port-side intake) airflow
	ICX7750-FAN-E	80-1007737-01	1	Fan kit of 4 fans; fan-side exhaust (port-side intake) airflow
	ICX7750-6Q	80-1007632-01	1	ICX 7750 with 6 40 GbE QSFP modules
IC7750 Config 2	ICX7750-48C	80-1007608-01	1	ICX 7750 with 48 1/10 GbE RJ-45 10GBASE-T ports, 6 40 GbE QSFP ports and modular interface slot. No power supplies or fan units (need to be ordered separately).
	RPS9E	80-1007870-01	2	500 W AC power supply; power-supply-side exhaust (port-side intake) airflow
	ICX7750-FAN-E	80-1007737-01	1	Fan kit of 4 fans; fan-side exhaust (port-side intake) airflow
	ICX7750-6Q	80-1007632-01	1	ICX 7750 with 6 40 GbE QSFP modules
IC7750 Config 3	ICX7750-26Q	80-1007609-01	1	ICX 7750 with 26 40 GbE QSFP ports and modular interface slot. No power supplies or fan units (need to be ordered separately).
	RPS9E	80-1007870-01	2	500 W AC power supply; power-supply-side exhaust (port-side intake) airflow
	ICX7750-FAN-E	80-1007737-01	1	Fan kit of 4 fans; fan-side exhaust (port-side intake) airflow
	ICX7750-6Q	80-1007632-01	1	ICX 7750 with 6 40 GbE QSFP modules

Table 7 - ICX 7750 Switch Family Part Numbers of Validated Cryptographic Modules

Figure 16 through Figure 20 illustrates an ICX 7750-48F cryptographic module

Figure 16 - Front/top side of the ICX 7750-48F

Figure 17 - Back side of the ICX 7750-48F with optional ICX7750-6Q module

Figure 18 - Left side of the ICX 7750-48F

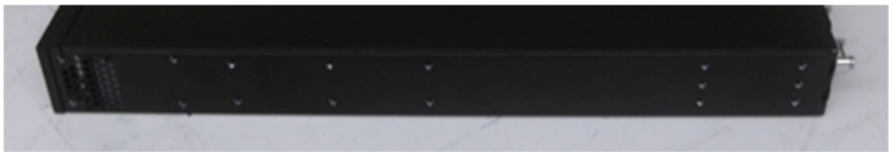

Figure 19 - Right side of the ICX 7750-48F

Figure 20 - Bottom side of the ICX 7750-48F

Figure 21 through Figure 25 illustrates an ICX 7750-48C cryptographic module

Figure 21 - Front/top side of the ICX 7750-48C

Figure 22 - Back side of the ICX 7750-48C with optional ICX7750-6Q module

Figure 23 - Left side of the ICX 7750-48C

Figure 24 - Right side of the ICX 7750-48C

Figure 25 - Bottom side of the ICX 7750-48C

Figure 26 through Figure 30 illustrates an ICX 7750-26Q cryptographic module

Figure 26 - Front/top side of the ICX 7750-26Q

Figure 27 - Back side of the ICX 7750-26Q with optional ICX7750-6Q module

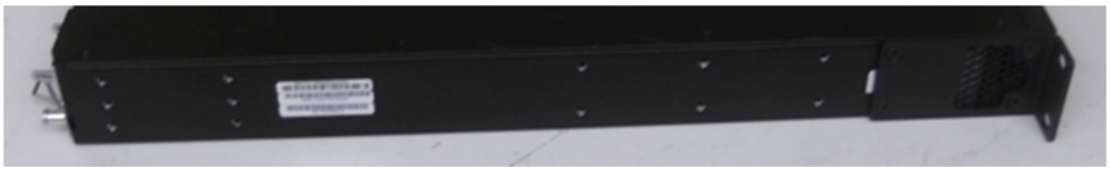

Figure 28 - Left side of the ICX 7750-26Q

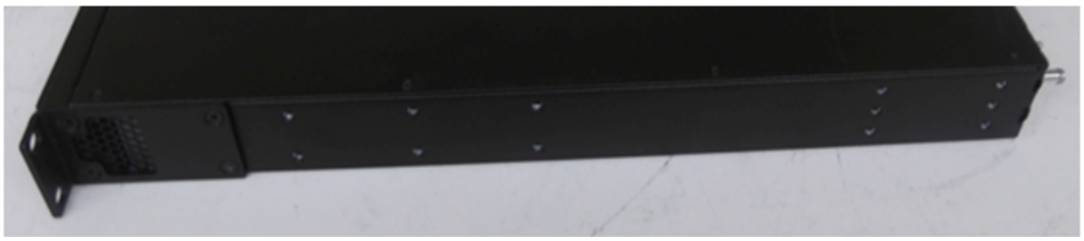

Figure 29 - Right side of the ICX 7750-26Q

Figure 30 - Bottom side of the ICX 7750-26Q

7 Ports and Interfaces

7.1 ICX 7150 Series

An ICX 7150 device provides network ports, management connectors, and status LED. This section describes the physical ports and the interfaces that provide for Data Input, Data Output, Control Input, and Status Output.

The ICX 7150 devices provide a range of physical network ports. The series supports both copper and fiber connectors. The ICX 7150 device has one RJ-45 network management port, one mini USB serial console port, and one USB storage port on the front panel.

Table 7 below shows the correspondence between the physical interfaces of an ICX 7150 device and the logical interfaces defined in FIPS 140-2.

Physical Port	Logical Interface
SFP+ ports	Data input/Data output, Status output
10/100/1000 Mbps RJ-45 ports	Data input/Data output, Status output
AC socket	Power
Console port (mini USB)	Control input, Status output
Management port	Control input, Status output
Reset	Control input
LED	Status output
USB type-A port	This port is permanently disabled

Table 8 - ICX 7150 Port mapping to logical interface

The Tables below summarize the physical port LED status provided by ICX 7150 devices.

LED	Condition	Status
Management Port (port status)	Flashing	There is traffic and packets are being transmitted and received.
	Steady	No traffic is being transmitted, but the link is active.
	Off	External cable is not present.
1/10 GbE 2.5/5G or 100/10 Mbps Port (RJ45 and SFP+)	Steady Green	Link is up in 10 GbE mode.
	Flashing Green	Link is up and packets are being transmitted or received.
	off	External cable is not connected

Table 9 - ICX 7150 Series Physical Port LED Status

LED	Condition	Status
PSU1,PSU2,PWR	Steady Green	Power Supply is on and operating normally.
	Steady Amber	Power supply fault.
	Off	Power is off or not present.

Table 10 - ICX 7150 Power (PSU1, PSU2, PWR) LED Status

LED State	Status of hardware
Steady Green	test successfully completed
Blinking Green	system self-test in progress
Off	switch did not perform Diag test in the most recent reload
Steady Amber	N/A
Blinking Amber	Diag test has detected a fault

Table 11 - ICX 7150 System DIAG Status

LED State	Status of hardware
Off	System is not powered ON
Steady Green	System is UP and running.
Blinking Green	Switch is initializing
Steady Amber	System is in boot mode
Blinking Amber	System is in crash state and watchdog timeout state Or System failed to boot into valid FI image

Table 12 - ICX 7150 System SYST Status

LED State	Status of hardware
Steady Green	- Stacking mode is enabled and switch is stack master
Blinking Green	- Stacking is initiating. Roles are being assigned.
Off	- Stack member /PE - Standalone
Steady Amber	- Stacking mode is enabled and switch is standby controller
Blinking Amber	- Stacking error- Switch in Non-op mode i.e., stacking is enabled but current unit not able to join stack to due to any stack related error condition i.e., o Image mismatch o Config Mismatch o License Mismatch - Losing master

Table 13 - ICX 7150 System MS Status

Note: Time line for the MS Led

The following is for a master:

1. Boot up, and begin to send probes if stack is enabled and the stack-ports are up (blinking green)
2. After it is elected as a master and finish hot swap other units, it shows steady green.
3. If any other unit joins, it temporarily shows blinking green until the unit is hot swapped.

The following is for a member or standby

1. Boot up, and begin to send probes if stack is enabled and the stack-ports are up (blinking green). If it never joins, the light is always blinking green.
2. After election finishes, there are a few possibilities:
    a. It is ready. The light is off (All non-master unit, including the standby, boots up as a member.)
    b. It is non-operational due to image/config/license mismatch. The light is blinking amber.
3. When a member is assigned a standby, the light changes from off to steady amber.
4. If the master is gone, a member will show blinking amber. The standby will take over and shows steady green.

LED State	Status of hardware
Steady Green	Steady green if successfully connected to the cloud management platform
Blinking Green	Blinking green if trying to connect to a cloud management platform
Off	Cloud management feature is disabled on the switch.
Steady Amber	Steady amber if failed to connect or could not reach the cloud. This is for intermediate connection issues only (which means the switch was connected to the cloud earlier)

Blinking Amber	Any critical error ■ If image upgrade is disrupted due to connectivity issue ■ switch not being able to connect to the cloud after a long period (TBD) of retry

Table 14 - ICX 7150 System CLD Status

7.2 ICX 7250 Series

An ICX 7250 device provides network ports, management connectors, and status LED. This section describes the physical ports and the interfaces that provide for Data Input, Data Output, Control Input, and Status Output.

The ICX 7250 devices provide a range of physical network ports. The series supports both copper and fiber connectors. The ICX 7250 device has one RJ-45 network management port, one mini USB serial console port, and one USB storage port on the front panel.

Table 14 below shows the correspondence between the physical interfaces of an ICX 7250 device and the logical interfaces defined in FIPS 140-2.

Physical Port	Logical Interface
SFP+ ports	Data input/Data output, Status output
10/100/1000 Mbps RJ-45 ports	Data input/Data output, Status output
AC socket	Power
Console port (mini USB)	Control input, Status output
Management port	Control input, Status output
Reset	Control input
LED	Status output
USB type-A port	This port is permanently disabled

Table 15 - ICX 7250 Port mapping to logical interface

The Tables below summarize the physical port LED status provided by ICX 7250 devices.

LED state	Status of hardware
On/Flashing green	The port has established a valid link at 10, 100 or 1000 Mbps. Flashing means the port is transmitting and receiving user packets.
Off	A link is not established with a remote port.

Table 16 ICX 7250 - RJ-45 port LEDs

LED state	Status of hardware
On/Steady green	Port is providing PoE power to a connected device.
Off	Port is not providing PoE power

Table 17 - ICX 7250 - 100/1000 Mbps RJ-45 PoE LEDs

LED state	Status of hardware
Off (no light)	The SFP port operates at 1 Gbps. Flashing indicates the port is transmitting and receiving user packets at 1 Gbps.
Off	A link is not established with a remote port.

Table 18 - ICX 7250 24G - SFP port LEDs

LED state	Status of hardware
On/Flashing Green	The SFP+ port is operating at 10 Gbps. Flashing indicates the port is transmitting and receiving user packets at 10 Gbps.
On/Flashing Yellow	The SFP+ port is operating at 1 Gbps. Flashing indicates the port is transmitting and receiving user packets at 1 Gbps.
Off	A link is not established with a remote host

Table 19 - ICX 7250 (except 24G) - 1/10 GbE SFP+ module port LEDs

LED state	Status of hardware
Green	Power supply is operating.
Yellow	Power supply fault.
Off	Power supply off

Table 20 - ICX 7250 – Power LEDs

LED state	Status of hardware
Green	EPS1 and EPS2 power supplies are operating normally.
Yellow	EPS1 and EPS2 power supply fault
Off	EPS1 and EPS2 off or not present

Table 21 - ICX 7250 – EPS1 and EPS2 port LEDs

LED state	Status of hardware
Flashing Green	System self-diagnostic test in progress. System reloads automatically
Steady Yellow	System self-diagnostic test has detected a fault. (Fan, thermal, or any interface fault.) The user must reload the system.

Table 22 - ICX 7250 - DIAG LED

LED state	Status of hardware
Green	The device is the Active controller. Flashing indicates the system is initializing
Yellow	Indicates the device is the Standby controller. Flashing indicates the system is in Master arbitration or selection state
Off	Device is operating as a stack member, or is in standalone mode

Table 23 - ICX 7250 - MS LED

LED state	Status of hardware
Green	Uplink port is operating normally
Off	Uplink has failed or there is no link

Table 24 - ICX 7250 - UPLINK LED

LED state	Status of hardware
Green	Downlink port is operating normally
Off	Downlink has failed or not present

Table 25 - ICX 7250 - DOWNLINK LED

LED state	Status of hardware
Green	Indicates stack unit identifier.

Table 26 - ICX 7250 - Stack ID LEDs

7.3 ICX 7750 Series

Each ICX 7750 device provides network ports, management connectors, and status LED. This section describes the physical ports and the interfaces that provide for Data Input, Data Output, Control Input, and Status Output.

The ICX 7750 devices provide a range of physical network ports. The series supports both copper and fiber connectors with some models supporting combination ports. Some models support uplink ports for stacking devices. Most models have a management port (also known as out-of-band management port; Gigabit Ethernet RJ-45 connector) and a console port (mini USB serial connector).

Table 27 shows the correspondence between the physical interfaces of an ICX 7750 device and the logical interfaces defined in FIPS 140-2.

Physical Port	Logical Interface
SFP ports	Data input/Data output, Status output
QSFP ports	Data input/Data output, Status output
10/100/1000 Mbps RJ-45 ports (see note 1)	Data input/Data output, Status output
AC socket	Power
External power supply connector	Power
Console port (mini USB)	Control input, Status output
Management port	Control input, Status output
Reset	Control input
LED	Status output
USB type-A port	This port is permanently disabled

Table 27 - ICX 7750 Port mapping to logical interface

Note: ICX 7750-26Q and ICX 7750-48F do not support 10/100/1000 Mbps RJ-45 ports

The Tables below summarize the physical port LED status provided by ICX 7750 devices.

LED	Condition	Status
Management Port (Left or Right)	Flashing	There is traffic and packets are being transmitted and received.
Management Port (Left or Right)	Steady	No traffic is being transmitted, but the link is active.
	Off	External cable is not present.
1/10 GbE Port (RJ45 and SFP+)	Steady Green	Link is up in 10 GbE mode.
	Flashing Green	There is 10 GbE activity (traffic) and packets are being transmitted or received.
	Steady Amber	Link is up in 1 GbE mode.
	Flashing Amber	There is 1 GbE activity (traffic) and packets are being transmitted or received.
40 GbE (rear port) front port LED	Off	Disabled.
	Steady Green	Link is up in 40 GbE mode.
	Flashing Green	Active traffic. Packets are being transmitted or received.
4x10 GbE (rear port) front port LED	Off	Disabled.
	Steady Amber	Link is up in 10 GbE mode.
	Flashing Amber	Active traffic. Packets are being transmitted or received.
10/100/1000 Mbps HA Ethernet port LEDs	Off	Not Cabled.
	Steady green	Link is up in 1 GbE mode.
	Blinking Green	There is 1 GbE traffic and packets are being transmitted or received.
	Steady Amber	Link is up in 10/100 Mbps mode.
	Blinking Amber	There is 10/100 Mbps traffic and packets are being transmitted or received.

Table 28 - ICX 7750 Series Physical Port LED Status

LED	Condition	Status
PSU1 and PSU2	Steady Green	PSU is on and operating normally.
	Steady Amber	PSU power supply fault.
	Off	PSU is off or not present.
Diag (Diagnostic)	Flashing Green	System self-diagnostic test in progress. System reloads automatically.
	Steady Amber	System self-diagnostic test has detected a fault.

	Steady Green	System self-diagnostic test completed successfully. Device reboots and turns the LED off.
	Off	Diagnostic is off.
MS LED	Off	Stacking mode is enabled and the switch is a stack member, or the switch is operating in stand-alone mode.

Table 29 - ICX 7750 System LED Status

LED	Condition	Status
MS LED	Steady Green	Stacking mode is enabled and the switch is the stack master.
	Steady Amber	Stacking mode is enabled and the switch is in slave mode.
HA LED	Off	System high-availability mode is disabled.
	Steady Green	System is operating in high-availability mode.
	Steady Amber	System is preparing to operate in high- availability mode.
RDNT LED	Off	System does not have redundant fans or PSUs installed.
	Steady Green	System is operating in redundant mode.
	Steady Amber	System has redundant fans and PSUs, but software has disabled redundant mode.

Table 30 - ICX 7750 Other LED Status

8 Modes of Operation

ICX 7150, 7250, and 7750 devices (aka FastIron cryptographic modules) have two modes of operation: FIPS Approved mode and non-Approved mode. Section 8.3 describes services and cryptographic algorithms available in FIPS-Approved mode. In non-FIPS Approved mode, the module runs without these FIPS policy rules applied. Section 10.3 FIPS Approved Mode describes how to invoke FIPS Approved mode.

8.1 Module Validation Level

The module meets an overall FIPS 140-2 compliance of Security Level 1

Security Requirements Section	Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A

Table 31 - Security Requirements and Levels

8.2 Roles

In FIPS Approved mode, the cryptographic modules support three (3) roles: Crypto Officer, Port Configuration Administrator and User Role:

1. Crypto Officer Role (Super User): The Crypto Officer Role on the device in FIPS Approved mode is equivalent to the administrator role super-user in non-FIPS mode. The Crypto Officer Role has complete access to the system. The Crypto Officer is the only role that can perform firmware loading.

2. Port Configuration Administrator Role (Port Configuration): The Port Configuration Administrator Role on the device in FIPS Approved mode is equivalent to a port configuration user in non- FIPS Approved mode. Hence, the Port Configuration Administrator Role has read-and-write access for configuring specific ports but not for global (system-wide) parameters.

3. User Role (Read-Only): The User Role on the device in FIPS Approved mode has read-only privileges and no configuration mode access (user).

The User role has read-only access to the cryptographic module while the Crypto Officer Role has access to all device commands. The cryptographic modules do not have a maintenance interface or maintenance role.

Section 9.2 describes the authentication policy for user roles.

8.3 Services

The services available to an operator depend on the operator's role. Unauthenticated operators may view externally visible status LED. LED signals indicate status that allows operators to determine if the network connections are functioning properly. Unauthenticated operators can also perform self-tests via a power-cycle. They can also view the module status by entering CLI "*`fips show`*" command.

For all other services, an operator must authenticate to the device as described in Section 9.2 Authentication. The cryptographic modules provide services for remote communication (SSHv2, SNMPv3 and Console) for management and configuration of cryptographic functions. The following subsections describe services available to operators based on role. Each description includes lists of cryptographic functions and critical security parameters (CSP) associated with the service. Table 32 summarizes the available FIPS Approved cryptographic functions.

Table 33 lists cryptographic functions that are Approved for use in FIPS Approved mode of operation.

Label	Cryptographic Algorithms	Cert.
AES	[FIPS 197] Advanced Encryption Algorithm Encryption, Decryption, MAC Generate & Verify Modes: ECB(128,192,256 bits)*, CBC(128,192,256 bits), CMAC(128 bits), CFB (128 bits), and CTR (128,192,256 bits) *Tested only as a prerequisite for other algorithms.	5022, 5024

	Please note that AES-KW (128 bits) was tested for AES #5022, but is not used.	
CVL	[SP 800-135] Application Specific Key Derivation Functions SNMPv3 KDF, SSHv2 KDF, TLSv1.0/1.1 KDF, TLSv1.2 KDF Please note that the CAVP and CMVP do not examine this module's implementations of the above protocols.	1567, 1569
DRBG	[SP 800-90A] Deterministic Random Bit Generators Variants: CTR DRBG with AES-256 (with PR and DF) Please note that HASH DRBG was tested for DRBG #1837, but is not used.	1837, 1839
DSA	[FIPS 186-4] Digital Signature Algorithm Key Generation* Size: DSA-2048 *DSA-2048 Key Generation was tested only as a prerequisite to Diffie Hellman key exchange (see "DH KA" in the table below). Please note that other operations have been tested but are not used. (Please refer to DSA Certs. #1318 and #1320 for details.)	1318, 1320
HMAC	[FIPS 198-1] Keyed-Hash Message Authentication code MAC Generate & Verify Variants: HMAC-SHA-1 (96, 160-bit tag) HMAC-SHA-256 (128, 192, 256-bit tags) HMAC-SHA-384 (192-bit tag)	3336, 3338
KTS	[SP800-38F §3.1] Functions: Key Wrap, Key Unwrap Variants: AES-128-CTR and HMAC-SHA-1 AES-256-CTR and HMAC-SHA-1 AES-128-CBC and HMAC-SHA-1 AES-128-CBC and HMAC-SHA-256 AES-256-CBC and HMAC-SHA-1 AES-256-CBC and HMAC-SHA-256 Key establishment methodology provides between 128 and 256 bits of encryption strength	AES #5022, #5024 HMAC #3336, #3338

RSA	[FIPS 186-4] Rivest Shamir Adleman Signature Algorithm Key Generation, Signature Generation, Signature Verification Sizes: RSA-1024*, RSA-2048 Hashes: SHA-1*, SHA-224, SHA-256, SHA-384, SHA-512 Padding Schemes: X9.31, PKCS 1.5, PSS *RSA-1024 is used for legacy signature verification only. SHA-1 is used for protocol-specific signature generation and legacy signature verification only. Please refer to RSA Certs. #2707 and #2709 for the exact keysize/hash/padding combinations supported.	2707, 2709
SHA	[FIPS 180-4] Secure Hash Algorithm (SHA-1*, SHA-224, SHA-256, SHA-384, SHA-512) Used for signature operations, as a component of other algorithms (e.g. HMAC, DRBG), password obfuscation, and other purposes *SHA-1 is only used for legacy signature verification, and for protocol-specific signature generation.	4081, 4083

Table 32 – FIPS Approved Cryptographic Algorithms allowed in FIPS Approved mode

Table 32 below lists all FIPS non-Approved Cryptographic Algorithms available in FIPS Approved Mode.

Label	Cryptographic Algorithms
KW	RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)
MD5	MD5 is used in the Approved mode for three purposes: • RADIUS obfuscated password output during operator authentication (this function is not exposed to the operator) • RADIUS server authenticity check (this function is not exposed to the operator) TLS v1.0/v1.1 KDF as per SP800-135 (this function is not exposed to the operator)
NDRNG	Generation of seeds for DRBG with an estimated entropy rate of 3.97 bits/ 8 bits (or greater, depending on model) and 128 bytes per function call
DH KA	Diffie-Hellman with safe primes [L=2048, N=2048] (key agreement; key establishment methodology provides 112 bits of encryption strength) using diffie-hellman-group-exchange-sha256

Table 33 - FIPS non-Approved Cryptographic Algorithms available in FIPS Approved Mode

Table 33 below, lists Roles, FIPS non-Approved Cryptographic Functions, Protocols, and Services only available in non-FIPS Approved Mode

Role	Service / Function	Description
This is not a user accessible service	HTTPS Cipher Suites	Hyper Text Transport Protocol in secure connection mode
Crypto Officer Role, User Role	HTTP	Hyper Text Transport Protocol (plaintext; no cryptography)
Crypto Officer Role, User Role	SSHv2	2-key Triple-DES (non-compliant), 3-key Triple-DES (non-compliant)
Crypto Officer Role, User Role	SNMP { Simple Network Management Protocol v1, v2 and v3 with MD5 / DES, AES (non-compliant) / SHA-1 (non-compliant) }	MD5 and DES, AES (non-compliant) / SHA-1 (non-compliant), SNMPv1, SNMPv2c and SNMPv3 (non-compliant) in noAuthNoPriv, authNoPriv modes Modes: DES in authPriv mode for SNMPV3 (non-compliant) Key sizes: DES 56 bits, AES-128 (non-compliant)
Crypto Officer Role	TFTP (Trivial File Transfer Protocol)	Trivial File Transfer Protocol (TFTP) is a file transfer protocol notable for its simplicity. It is generally used for automated transfer of configuration or boot files between machines in a local environment. Compared to FTP, TFTP is extremely limited, providing no authentication, and is rarely used interactively by a user. Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)
This is not a user accessible service	“Two way encryption”	Base64
This is not a user accessible service	MD5	Message Digest 5 algorithm is used as cryptographic hash function to check for verification of data integrity and wide variety of cryptographic applications Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)

Role	Service / Function	Description
Crypto Officer Role, User Role	Syslog	Syslog is a standard for message logging. It permits separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)
Crypto Officer Role, User Role	VSRP	Virtual Switch Redundancy Protocol Modes: Layer 2 mode Key sizes: Not Applicable (plaintext; no cryptography)
Crypto Officer Role, User Role	VRRP/VRRP-E	Virtual Router Redundancy Protocol (VRRP) and Virtual Router Redundancy Protocol (VRRP-E) Enhancement Modes: Layer 3 mode Key sizes: Not Applicable (plaintext; no cryptography)
Crypto Officer Role, User Role	MSTP	Multiple Spanning Tree Protocol Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)
Crypto Officer Role, User Role	NTP (Authentication using MD5)	Network Time Protocol Modes: MD5 and SHA-1 (non-compliant) for authentication Key sizes: 20 bytes
Crypto Officer Role, User Role	BGP	Border Gateway Protocol (BGP) is a standardized exterior gateway protocol. Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)
This is not a user accessible service	AES-192 (non-compliant)	AES-192 (non-compliant) encryption/decryption is only available in non-FIPS mode
This is not a user accessible service	DSA (non-compliant)	DSA (non-compliant) digital signature generation/verification only available in non- FIPS mode

Table 34 - Roles, FIPS non-Approved Cryptographic Functions and Protocols only available in non-FIPS Approved Mode

Note: In addition to Table 33, all algorithms in Tables 31 and 32 are available in the non-Approved mode, but are not compliant with the usual applicable standards.

8.4 User Role Services

8.4.1 SSHv2

This service provides a secure session between the cryptographic module and an SSHv2 client using SSHv2 protocol. The cryptographic module authenticates an SSHv2 client and provides an encrypted communication channel. An operator may use an SSHv2 session for managing the device via the command line interface.

The cryptographic modules support three (3) kinds of SSHv2 client authentication: password, client public key and keyboard interactive. For password authentication, an operator attempting to establish an SSHv2 session provides a password through the SSHv2 client. The cryptographic module authenticates operator with passwords stored on the device, on a RADIUS server. Section 9.2 Authentication provides authentication details.

The keyboard interactive (KI) authentication goes one step ahead. It allows multiple challenges to be issued by the cryptographic module, using the backend RADIUS server, to the SSHv2 client. Only after the SSHv2 client responds correctly to the challenges, will the SSHv2 client get authenticated and proper access is given to the cryptographic module.

SSHv2 supports Diffie-Hellman (DH) to configure the modulus size on the SSHv2 server for the purpose of key- exchange.

Maximum number of concurrent SSHv2 user sessions supported is five (5).

The following encryption algorithms are available for negotiation during the key exchange with an SSHv2 client:

- AES-CTR with a 128-bit key (aes128-ctr),
- AES-CTR with a 256-bit key (aes256-ctr),

All secure hashing is done with HMAC-SHA-1.

The following MAC algorithms are available for negotiation during the key exchange with an SSHv2 client: (hmac-sha1) HMAC-SHA1 (digest length = key length = 20 bytes)

In User role access, the client is given access to three (3) commands: *`enable`*, *`exit`* and *`terminal`*. The `enable` command allows user to re-authenticate using a different role. If the role is the same, based on the credentials given during the *`enable`* command, the user has access to a small subset of commands that can perform *`ping`* *`traceroute`* in addition to *`show`* commands.

8.4.2 SNMP

SNMPv1 and SNMPv2 services are disabled in FIPS mode and the SNMPv3 service with authentication as HMAC-MD5 and privacy as DES are also disabled (only HMAC-SHA-1 and AES-CFB are used). The SNMPv3 service within User role allows read-only access to the SNMP MIB within the FastIron device. The device does not provide SNMP MIB access to CSPs when operating in FIPS Approved mode. All other MIB objects are made available for use in approved FIPS mode. These other MIB objects provide capability to monitor the various functional entities in the module which are non-security relevant.

8.4.3 Console

Console connection occurs via a directly connected RS-232 serial cable. Once authenticated as the User, the module provides console commands to display information about a FastIron cryptographic module and perform basic tasks (such as pings). The User role has read-only privileges and no configuration mode access. The list of commands available is the same as the list mentioned in the SSHv2 service.

8.4.4 NTP

The NTP [same as NTPv4] Network Time Protocol configuration and time statistics details can be viewed but not configured.

8.5 Port Configuration Administrator Role Services

8.5.1 SSHv2

This service is described in Section 8.4.1 above.

The Port Configuration Administrator will have seven commands, which allows this user to run show commands, run ping or trace route. The `enable` command allows the user to re-authenticate as described in Section 8.4.1. Within the configuration mode, this role provides access to all the port configuration commands, e.g., all sub-commands within “interface eth 1/1” command. This operator can transfer and store firmware images and configuration files between the network and the system, and review the configuration.

8.5.2 SNMP

The SNMP service is not available for a Port Configuration Administrator Role Service.

8.5.3 Console

This service is described in Section 8.4.3 above. Console access as the Port Configuration Administrator provides an operator with the same capabilities as User Console commands plus configuration commands associated with a network port on the device. EXEC commands. The list of commands available is the same as those mentioned in the SSHv2 service.

8.5.4 NTP

The NTP [same as NTPv4] Network Time Protocol configuration and time statistics details can be viewed but not configured.

8.6 Crypto Officer Role Services

8.6.1 SSHv2

In addition to the two methods of authentication, password and keyboard interactive, described in Section 8.4.1, SSHv2 service in this role supports RSA public key authentication, in which the device stores a collection of client public keys. Only clients with a private key that corresponds to one of the stored public keys can gain access to the device using SSHv2. After a client presents a public key which matches one of the stored CO SSHv2 public keys, and provides a corresponding signature, the device will give Crypto Officer access to the entire module.

The Crypto Officer has full read and write access to the cryptographic module.

When firmware download is desired, the Crypto Officer shall download firmware download in the primary image and secondary image.

The Crypto Officer can perform zeroization by invoking the firmware command "`fips zeroize all`" or session termination.

8.6.2 SCP

This is a secure copy service. The service supports both outbound and inbound copies of configuration, binary images, or files. Binary Images can be copied and installed similar to TFTP operation (that is, upload from device to host and download from host to device, respectively). SCP automatically uses the authentication methods, encryption algorithm, and MAC algorithm configured for SSHv2. For example, if password authentication is enabled for SSHv2, the user is prompted for a user name and password before SCP allows a file to be transferred. One use of SCP on the cryptographic modules is to copy user digital certificates and host public-private key pairs to the device in support of HTTPS. Other use could be to copy configuration to/from the cryptographic module.

8.6.3 SNMP

This service is described in Section 8.4.2 above. The SNMP service within Crypto Officer Role allows read- write access to only Non-Security Relevant elements of the SNMP MIB within the FastIron device.

8.6.4 Console

Logging in through the CLI service is described in Section 8.4.3 above. Console commands provide an authenticated Crypto Officer complete access to all the commands within the cryptographic module. This operator can enable, disable and perform status checks. This operator can also enable any service by configuring the corresponding command. For example, to turn on SSHv2 service, the operator creates a pair of RSA host keys, to configure the authentication scheme for SSHv2 access; afterwards the operator may securely import additional pairs of RSA host keys as needed over a secured SSHv2 connection. To enable the Web Management service, the operator would securely import a pair of RSA host keys and a digital certificate using corresponding commands (over a secured SSHv2 connection), and enable the HTTPS server.

NOTE: The cryptographic module "does not" support DSA key generation in FIPS mode, except as part of Diffie Hellman.

8.6.5 NTP

The NTP [same as NTPv4] Network Time Protocol can be configured to provide cryptographic authentication of messages with the clients/peers, and with its upstream time server. Symmetric key scheme is supported for authentication.

NTPv4 specification (RFC-5905), allows any one of possibly 65,534 message digest keys (excluding zero), each distinguished by a 32-bit key ID, to authenticate an association. The servers and clients involved must agree on the key ID, key type and key to authenticate NTP packets.

NTP service with MD5 key authentication is disabled in FIPS mode.

NTPv4 service with SHA1 key authentication is available upon configuration in FIPS mode. This is not a cryptographic service

9 Policies

9.1 Security Rules

The cryptographic module's design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the FIPS 140-2 Level 1 security requirements. After configuring a FastIron device to operate in FIPS Approved mode, the Crypto Officer must execute the "fips self-tests" command to validate the integrity of the firmware installed on the device. If an error is detected during the self-test, the error must be corrected prior to rebooting the device. These self-tests are automatically run upon module power-up each time when the device is in FIPS mode.

1) The cryptographic module provides role-based authentication.

2) Until the module is placed in a valid role, the operator does not have access to any Critical Security Parameters (CSPs).

3) The cryptographic module performs the following tests:

    a) Power up Self-Tests:

        i) Cryptographic Known Answer Tests (KAT):

            (1) AES-128,192,256-bit key sizes KAT (encrypt) in CBC, ECB, CTR and CFB modes*

            (2) AES-128,192,256-bit key sizes KAT (decrypt) in CBC, ECB, CTR and CFB modes*

            (3) SHA-1,256,384,512 KAT (Hashing)

            (4) HMAC-SHA-1,256 KAT (Hashing)

            (5) RSA 2048 bit key size KAT (encrypt)

            (6) RSA 2048 bit key size KAT (decrypt)

(7) RSA 2048 bit key size, SHA-256,384,512 Hash KAT (signature generation)

(8) RSA 2048 bit key size, SHA-256,384,512 Hash KAT (signature verification)

(9) DRBG KAT (CTR_DRBG) and Health Tests

(10) SP800-135 TLS v1.0 KDF KAT (CVL #1567)

(11) SP800-135 SSHv2 KDF KAT (CVL #1567)

(12) SP800-135 TLS v1.2 KDF KAT (CVL #1567)

(13) SP800-135 SNMPv3 KDF KAT (CVL #1567)

(14) AES-CMAC KAT

(15) Diffie-Hellman KAT (Primitive "Z" computation)

ii) Firmware Integrity Test (CRC 32) [run in FIPS mode and non-FIPS mode]

iii) If the module does not detect an error during the Power on Self-Test (POST), at the conclusion of the test, the console displays the message shown below.

```
Crypto module initialization and Known Answer Test (KAT) Passed
```

iv) If the module detects an error during the POST, at the conclusion of the test, the console displays the message shown below. After displaying the failure message, the module reboots.

```
Crypto Module Failed < Reason String >
```

b) Conditional Self-Tests:

i) Continuous Random Number Generator (RNG) test – performed on NDRNG

ii) Continuous Random Number Generator test – performed on DRBG

iii) RSA 2048 SHA-256 Pairwise Consistency Test (Sign/Verify)

iv) RSA 2048 SHA-256 Pairwise Consistency Test (Encrypt/Decrypt)

v) Firmware Load Test: RSA 2048 bit, SHA-256 Signature Verification

vi) Alternating Bypass Test

vii) Manual Key Entry Test: N/A

viii) ECDSA Pairwise Consistency Test (Sign/Verify)

4) At any time the cryptographic module is in an idle state, the operator can command the module to perform the power-up self-test by executing the "`fips self-tests`" command.

5) Data output to services defined in Section 8.3 Services is inhibited during key generation, self-tests, zeroization, and error states.

6) Status information does not contain CSPs or sensitive data that if used could compromise the module.

7) As per FIPS 140-2 Implementation Guidance D.11, the following protocols have not been reviewed or tested by the CAVP or CMVP:
   a) TLS v1.0/1.1
   b) SSHv2
   c) TLS v1.2
   d) SNMPv3

9.1.1 FIPS Fatal Cryptographic Module Failure

When POST is successful, the following messages will be displayed on the console:

```
FIPS Power On Self Tests and KAT tests successful.
Running continuous DRBG check.
Running continuous DRBG check successful.
Pairwise consistency check successful.
fips crypto drbg health check tests ran successful.
Crypto module initialization and Known Answer Test (KAT) Passed.
```

In order to operate a cryptographic module securely, an operator should be aware of the following rules for FIPS Approved mode of operation:

External communication channels / ports are not available before initialization of the cryptographic module.

The cryptographic module uses a FIPS Approved random number generator, CTR_DRBG.

The cryptographic modules shall use FIPS Approved key generation methods:

1) RSA public and private keys in accordance with [ANSI X9.31]

The cryptographic modules shall use Approved (or allowed) key establishment techniques:

1) Diffie-Hellman
2) RSA Key Wrapping
3) AES Key Wrapping

The cryptographic modules shall restrict key entry and key generation to authenticated roles.

The cryptographic modules shall not display plaintext secret or private keys. The device shall display "…" in place of plaintext keys.

The cryptographic module uses automated methods to establish session keys for SSHv2. The cryptographic module only performs “get” operations using SNMP.

9.2 Authentication

The cryptographic modules support role-based authentication. A device can perform authentication and authorization (that is, role selection) using RADIUS and local configuration database. Moreover, the cryptographic modules support multiple authentication methods for each service.

For first-time access, an operator can authenticate without a password. To implement one or more authentication methods for securing access to the device, an operator in the Crypto Officer Role configures authentication-method lists that set the order in which a device consults authentication methods. In an authentication-method list, an operator specifies an access method (Console, SSHv2, Web and SNMP) and the order in which the device tries one or more of the following authentication methods:

1) Line Password Authentication,
2) Enable Password Authentication,
3) Local User Authentication,
4) RADIUS Authentication with exec authorization and command authorization, and
5) Pre-shared keys

When a list is configured, the device attempts the first method listed to provide authentication. If that method is not available, (for example, the device cannot reach a RADIUS server) the device tries the next method until a method in the list is available or all methods have been tried.

The cryptographic modules allow multiple concurrent operators through SSHv2 and the console, only limited by the system resources.

9.2.1 Line Password Authentication Method

The Line Password Authentication method uses the Telnet password to authenticate an operator.

To use Line Password Authentication, a Crypto Officer must set the Telnet password. Please note that when operating in FIPS mode, Telnet is disabled and Line Password Authentication is not available.

9.2.2 Enable Password Authentication Method

The Enable Password Authentication Method uses a password corresponding to each role to authenticate an operator. An operator must enter the read-only password to select the User role. An operator enters the port-config password to select the Port Configuration Administrator role. An operator enters the super-user password to select the Crypto Officer Role.

To use Enable Password Authentication, a Crypto Officer must set the password for each privilege level.

9.2.3 Local Password Authentication Method

The Local Password Authentication Method uses a password associated with a user name to authenticate an operator. An operator enters a user name and corresponding password. The cryptographic modules assign the role associated with the user name to the operator when authentication is successful.

To use Local Password Authentication, a Crypto Officer must define user accounts. The definition includes a user name, password, and privilege level (which determines role).

9.2.4 RADIUS Authentication Method

The RADIUS Authentication method uses one or more RADIUS servers to verify user names and passwords. The cryptographic modules prompt an operator for user name and password. The device sends the user name and password to the RADIUS server. Upon successful authentication, the RADIUS server returns the operator's privilege level, which determines the operator's role. If a RADIUS server does not respond, the cryptographic module will send the user name and password information to the next configured RADIUS server.

The cryptographic modules support additional command authorization with RADIUS Authentication. The following events occur when RADIUS command authorization takes place.

1) A user previously authenticated by a RADIUS server enters a command on the cryptographic module.
2) The cryptographic module looks at its configuration to see if the command is at a privilege level that requires RADIUS command authorization.
3) If the command belongs to a privilege level that requires authorization, the FastIron cryptographic modules looks at the list of commands returned to it when RADIUS server authenticated the user.

NOTE: After RADIUS authentication takes place, the command list resides on the cryptographic module. The device does not consult the RADIUS server again once the operator has been authenticated. This means that any changes made to the operator's command list on the RADIUS server are not reflected until the next time the RADIUS server authenticates the operator, and the server sends a new command list to the cryptographic module.

To use RADIUS authentication, a Crypto Officer must configure RADIUS server settings along with authentication and authorization settings.

9.2.5 Strength of Authentication

This section describes the strength of each authentication method.

9.2.5.1 All roles

All users can utilize all other available authentication techniques for the purpose of authentication.

The cryptographic modules minimize the likelihood that a random authentication attempt will succeed. The module supports minimum eight (8) character passwords selected from the following character set: digits (Qty. 10), lowercase (Qty. 26) and uppercase (Qty. 26) letters, and punctuation marks (Qty. 18) in passwords. Therefore the probability of a random attempt is 1/ 80^8 which is less than 1/1,000,000.

The module enforces a one second delay for each attempted password verification, therefore maximum of 60 attempts per minute, thus the probability of multiple consecutive attempts within a one minute period is 60/80^8 which is less than 1/100,000.

The probability of a successful random guess of a RADIUS password during a one-minute period is less than three (3) in 1,000,000 which is less than 1/100,000 as the authentication message needs to go to the server from the switch and then the response needs to come back to the switch.

For the SNMPv3 secret used for authentication, the module supports minimum eight (8) character passwords selected from the following character set: digits (Qty. 10), lowercase (Qty. 26) and uppercase (Qty. 26) letters, and punctuation marks (Qty. 18) in passwords. Therefore the probability of a random attempt is 1/ 80^8 which is less than 1/1,000,000.

The module can process one (1) authentication packet per 10 msec. Therefore, the probability of multiple consecutive attempts within a one minute period is 6000/80^8 which is less than 1/100,000.

For the SNMPv3 secret used for privacy, the module supports minimum 12 character passwords selected from the following character set: digits (Qty. 10), lowercase (Qty. 26) and uppercase (Qty. 26) letters, and punctuation marks (Qty. 18) in passwords. Therefore the probability of a random attempt is 1/ 80^12 which is less than 1/1,000,000.

The module can process one (1) authentication packet per 10 msec. Therefore, the probability of multiple consecutive attempts within a one minute period is 6000/80^12 which is less than 1/100,000.

For the NTP secret, the module supports minimum eight (8) character passwords selected from the following character set: digits (Qty. 10), lowercase (Qty. 26) and uppercase (Qty. 26) letters, and punctuation marks (Qty. 18) in passwords. Therefore the probability of a random attempt is 1/ 80^8 which is less than 1/1,000,000.

The module can process one (1) authentication packet per 10 msec. Therefore, the probability of multiple consecutive attempts within a one minute period is 6000/80^8 which is less than 1/100,000.

9.2.6 Pre-shared keys Method

The table below summarizes the access operators in each role have to critical security parameters. The table entries have the following meanings:

1) r – Operator can read the value of the item,
2) w - Operator can write a new value for the item,
3) x - Operator can use the value of the item without direct access (for example encrypt with an encryption key)
4) d - Operator can delete the value of the item (zeroize).

Roles & Services / CSPs & Public Keys	User Role				Port Configuration Administrator				Crypto Officer Role				
	SSHv2	SNMP	Console	NTP	SSHv2	SNMP	Console	NTP	SSHv2	SCP	SNMP	Console	NTP
SSHv2 Host RSA Private Key (2048 bit)	x				x				xwd	x		wd	
SSHv2 DH Private Key (2048 bit)	x				x				xwd	x		wd	
SSHv2 DH Shared Secret Key (2048 bit)	x				x				wxd	x		wxd	
SSHv2/SCP Session Keys (128 and 256 bit AES-CTR)	x				x				wxd	x		wxd	
SSHv2/SCP Authentication Key (160-bits HMAC-SHA-1)	x				x				wxd	x		wxd	
SSHv2 KDF Internal State	x				x				wxd	x		wxd	
TLS Client RSA Private Key (RSA 2048 bit)									rwxd			rwxd	
TLS Pre-Master Secret					x				wxd				
TLS Master Secret					x				wxd				
TLS Encryption Keys					x				wxd				
TLS Authentication Keys					x				wxd				
DRBG Entropy Input	x				x				wxd	x		wxd	
CTR_DRBG Internal State	x	x	x		x	x	x		wxd	x	x	x	
User Password	x	x	x						xrwd	xrwd		xrwd	
Port Administrator Password					x	x	x		xrwd	xrwd		xrwd	
Crypto Officer Password									xrwd	xrwd	x	xrwd	
RADIUS Secret	x		x		x		x		xrwd	xrwd		xrwd	
SNMPv3 secret	r	r	r		r	r	r		rwd	rwd	r	rwd	

Roles & Services / CSPs & Public Keys	User Role				Port Configuration Administrator				Crypto Officer Role				
	SSHv2	SNMP	Console	NTP	SSHv2	SNMP	Console	NTP	SSHv2	SCP	SNMP	Console	NTP
NTP secret	r			r	r		r	r	rwd	rwd	r	rw	rwd
Firmware Integrity / Firmware Load RSA Public Key								xd	x				
SSHv2 Host RSA Public key	rx				rx				xrwd	xrw		rwd	
SSHv2 Client RSA Public Key	rx				rx				xrwd	xrwd		xrwd	
SSHv2 DH Public Key	rx				rx			xd	xrwd				
SSHv2 DH Peer Public Key	wx				wx			xd	xrwd				
TLS Client Public Key (RSA 2048 bit)					x				rwd			rwd	
TLS Peer Public Key (RSA 2048 bit)					x				rwd			Rwd	

9.2.7 CSP Zeroization

All CSPs can be zeroized by executing the "`fips zeroize all`" command. This command can be executed via the Console and SSHv2 service.

10 Description of FIPS Approved Mode

This section describes:

A. FIPS Approved mode, Section 10.1, describes:
    - This section describes required actions before you can use the module in FIPS Approved mode of operation
    - The nature of operational conditions in the module while operating in FIPS Approved mode.
B. Displaying mode status, Section 10.2, provides details on how to examine the status for the module's mode of operation.
C. Invoking FIPS approved mode, Section 10.3, describes the required steps in order to invoke the FIPS approved mode on the module.

10.1 FIPS Approved Mode

This section describes FIPS Approved mode of operation and the sequence of actions that places a FastIron cryptographic module in FIPS Approved mode.

FIPS Approved mode disables the following:

1) Telnet access including the telnet server command
2) Command `ip ssh scp disable`
3) TFTP access
4) SNMP access to CSP MIB objects
5) Access to all commands within the monitor mode
6) Port 280

Entering FIPS Approved mode also clears:

1) Protocol shared secret and host passwords
2) SSHv2 RSA host keys

FIPS Approved mode enables:

1) SCP

10.2 Displaying Mode Status

The cryptographic modules provide the *fips show* command to display status information about the device's FIPS mode. This command displays information about the policy settings. This information includes the status of administrative commands for security policy, the status of security policy enforcement and security policy settings.

The *fips enable* command changes the status of administrative commands; see also Section 10.1, FIPS Approved Mode.

The following example shows the output of the *fips show* command before an operator enters the *fips enable* command. Displayed status information indicates that administrative commands for security policy are unavailable (Administrative Status is OFF) and the device is not enforcing a security policy (Operational Status is OFF).

```
FIPS mode: Administrative Status: OFF, Operational Status: OFF
```

The following example shows the output of the *fips show* command after an operator enters the *fips enable* command. Displayed status information indicates that administrative commands for security policy are available (Administrative Status is ON) but the device is not enforcing a security policy yet (Operational Status is OFF).

```
FIPS mode: Administrative Status: ON, Operational Status: OFF
Some shared secrets inherited from non-Approved mode may not be fips
compliant and has to be zeroized. The system needs to be reloaded to operate
in FIPS mode.
System Specific:
OS monitor mode access: Disabled
Management Protocol Specific:
Telnet server: Disabled
TFTP Client: Disabled
HTTPS SSL 3.0: Disabled
SNMP Access to security objects: Disabled
Critical Security Parameter Updates across FIPS Boundary:
Protocol shared secret and host passwords: Clear
SSHv2 RSA Host Keys: Clear
```

The following example shows the output of the *fips show* command after the device reloads successfully in the default strict FIPS mode. Displayed status information indicates that administrative commands for security policy are available (Administrative Status is ON) and the device is enforcing a security policy (Operational Status is ON).

```
FIPS mode: Administrative Status: ON, Operational Status: ON
System Specific:
OS monitor mode access: Disabled
Management Protocol Specific:
Telnet server: Disabled
TFTP Client: Disabled
HTTPS SSL 3.0: Disabled
SNMP Access to security objects: Disabled
Critical Security Parameter Updates across FIPS Boundary:
Protocol shared secret and host passwords:   Clear
SSHv2 RSA Host Keys: Clear
```

10.3 Invoking FIPS Approved Mode

Crypto Officer may use "FastIron FIPS and Common Criteria Configuration Guide" documentation on ruckuswireless.com for configuration of these devices.

To invoke the FIPS Approved mode of operation, perform the following steps:

1) Assume Crypto Officer role.
2) Enter command: *fips enable*

   The device enables FIPS administrative commands. The device is not in FIPS Approved Mode of operation yet. Do not change the default strict FIPS security policy, which is required for FIPS Approved mode.

3) Enter command: *fips zeroize all*

   The device zeros out the shared secrets used by various networking protocols including host access passwords, SSHv2 host keys, and HTTPS host keys with the digital signature. This will delete all the users.

4) Enter command: *no web-management hp-top-tools*

   The device will turn off access by HP ProCurve Manager via port 280.

5) Generate the SSHv2 Host RSA Private Key (2048 bit) and SSHv2 Host RSA Public Key.

   a) Use CLI command: *crypto key generate*

6) Generate the TLS Host RSA Private Key (RSA 2048 bit) and TLS Host Public Key (RSA 2048 bit).

a) Use CLI command: *crypto-ssl certificate generate*

NOTE: The command syntax above includes the nomenclature "ssl" from a legacy command line API; for the avoidance of doubt it is hereby stated that such syntax is a misnomer as SSL "IS NOT" supported in FIPS mode (i.e., the cryptographic module enforces the use of TLS in FIPS mode; SSL "IS NOT" supported in FIPS mode)

7) Copy signature files of all the affected images to the flash memory.

   a) Use CLI command: *scp <syntax>*

8) Create a new user

   a) Use user command: *user <username> password <password>*

9) Enter command: *write memory*.

   The device saves the running configuration as the startup configuration.

10) Enter command: *reload*

    The device resets and begins operation in FIPS Approved mode.
    (**NOTE**: Do not press B as the module is reloading).

11) Enter command: *fips show* (This command displays the FIPS-related status, which should confirm the security policy is the default security policy.)

11 Glossary

Term/Acronym	Description
AES	Advanced Encryption Standard
CBC	Cipher-Block Chaining
CLI	Command Line Interface
CSP	Critical Security Parameter
DES	Data Encryption Standard
DF	Derivation Function (for SP800-90A DRBG)
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECB	Electronic Codebook mode
FI	FastIron
GbE	Gigabit Ethernet
HMAC	Keyed-Hash Message Authentication Code
KDF	Key Derivation Function
LED	Light-Emitting Diode
Mbps	Megabits per second
NDRNG	Non-Deterministic Random Number Generator
POE	Power over Ethernet
POE+	High Power over Ethernet
PR	Prediction Resistance (for SP800-90A DRBG)
RADIUS	Remote Authentication Dial in User Service
RSA	Rivest Shamir Adleman
SCP	Secure Copy
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSHv2	Secure Shell
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security

Table 35 - Glossary

12 Appendix A: Critical Security Parameters

The module supports the following CSPs and public keys:

12.1 SSHv2 & SCP

1. SSHv2 Host RSA Private Key (2048 bit)
   - Description: Used to authenticate SSHv2 server to client
   - Type: RSA-2048 Private Key
   - Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method.
   - Establishment: N/A
   - Entry: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
   - Output: N/A
   - Storage: Plaintext in RAM and BER encoded (plaintext) in Compact Flash
   - Key-to-Entity: Process
   - Zeroization: "fips zeroize all" command

2. SSHv2 DH Private Key (2048 bit)
   - Description: Used in SCP and SSHv2 to establish a shared secret
   - Type: DH-2048 Private Key
   - Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the finite field is the output of the SP800-90A DRBG; allowed method as per FIPS 140-2 IG D.8 Scenario 4
   - Establishment: N/A
   - Entry: N/A
   - Output: N/A
   - Storage: Plaintext in RAM
   - Key-to-Entity: Process
   - Zeroization: Session termination and "fips zeroize all" command

3. SSHv2 DH Shared Secret Key (2048 bit)
   - Description: Output from the DH Key agreement primitive - (K) and (H). Used in SSHv2 KDF to derive (client and server) session keys.
   - Type: DH Shared Secret
   - Generation: N/A
   - Establishment: SSHv2 DH Key Agreement; allowed method as per FIPS 140-2 IG D.8 Scenario 4
   - Entry: N/A
   - Output: N/A
   - Storage: Plaintext in RAM
   - Key-to-Entity: User
   - Zeroization: Session termination and "fips zeroize all" command

4. SSHv2/SCP Session Keys (128 and 256 bit AES-CTR)
   - Description: AES encryption key used to secure SSHv2/SCP
   - Type: AES-128-CTR or AES-256-CTR Key

- Generation: N/A
- Establishment: SSHv2 DH Key Agreement and SSHv2 KDF (SP800-135 Section 5.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: User
- Zeroization: Session termination and "fips zeroize all" command

5. SSHv2/SCP Authentication Key (160 bits HMAC-SHA-1)
   - Description: Session authentication key used to authenticate and provide integrity of SSHv2 session
   - Type: HMAC-SHA-1
   - Generation: N/A
   - Establishment: SSHv2 DH Key Agreement and SSHv2 KDF (SP800-135 Section 5.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4
   - Entry: N/A
   - Output: N/A
   - Storage: Plaintext in RAM
   - Key-to-Entity: User
   - Zeroization: Session termination and "fips zeroize all" command

6. SSHv2 KDF Internal State
   - Description: Used to generate Host encryption and authentication key
   - Type: KDF
   - Generation: N/A
   - Establishment: SSHv2 DH Key Agreement and SSHv2 KDF (SP800-135 Section 5.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4
   - Entry: N/A
   - Output: N/A
   - Storage: Plaintext in RAM
   - Key-to-Entity: User
   - Zeroization: Session termination and "fips zeroize all" command

12.2 TLS

7. TLS Client RSA Private Key (RSA 2048 bit)
   - Description: RSA key used to establish TLS v1.0/1.1 and v1.2 sessions
   - Type: RSA-2048 Private Key
   - Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method.
   - Establishment: N/A
   - Entry: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
   - Output: N/A
   - Storage: Plaintext in RAM and BER encoded (plaintext) in Compact Flash
   - Key-to-Entity: Process
   - Zeroization: "fips zeroize all" command

8. TLS Pre-Master Secret
   - Description: Secret value used to establish the TLS Master Secret
   - Type: TLS key precursor
   - Generation: None
   - Establishment: Diffie-Hellman exchange; allowed as per FIPS 140-2 IG D.8.
   - Entry: N/A
   - Output: N/A
   - Storage: Plaintext in RAM
   - Key-to-Entity: User
   - Zeroization: Session termination and "fips zeroize all" command

9. TLS Master Secret
   - Description: 48 bytes secret value used to establish the TLS Encryption Keys and TLS Authentication Keys
   - Type: TLS v1.0/1.1 and v1.2 shared secret
   - Generation: N/A
   - Establishment: TLS KDF as per SP800-135 Section 4.2.1 & 4.2.2; allowed method as per FIPS 140-2 IG D.8 Scenario 4
   - Entry: N/A
   - Output: N/A
   - Storage: Plaintext in RAM
   - Key-to-Entity: User
   - Zeroization: Session termination and "fips zeroize all" command

10. TLS Encryption Keys
   - Description: AES keys used to encrypt TLS session data
   - Type: AES-CBC-128 or AES-CBC-256
   - Generation: N/A
   - Establishment: TLS KDF as per SP800-135 Section 4.2.1 & 4.2.2; allowed method as per FIPS 140-2 IG D.8 Scenario 4
   - Entry: N/A
   - Output: N/A
   - Storage: Plaintext in RAM
   - Key-to-Entity: User
   - Zeroization: Session termination and "fips zeroize all" command

11. TLS Authentication Keys
   - Description: HMAC keys used to authenticate TLS session data
   - Type: HMAC-SHA-1 (all TLS versions) or HMAC-SHA-256 (TLSv1.2 only)
   - Generation: N/A
   - Establishment: TLS KDF as per SP800-135 Section 4.2.1 & 4.2.2; allowed method as per FIPS 140-2 IG D.8 Scenario 4.
   - Entry: N/A
   - Output: N/A
   - Storage: Plaintext in RAM
   - Key-to-Entity: User

- Zeroization: Session termination and "fips zeroize all" command

12.3 Random Number Generation

12. DRBG Entropy Input
    - Description: Entropy Input for the SP800-90A CTR_DRBG
    - Type: DRBG Seed material
    - Generation: internally generated; raw random data from NDRNG
    - Establishment: N/A
    - Entry: N/A
    - Output: N/A
    - Storage: Plaintext in RAM
    - Key-to-Entity: Process
    - Zeroization: Power cycle and "fips zeroize all" command

13. DRBG Internal State
    - Description: Internal State of SP800-90A CTR_DRBG (V and Key)
    - Type: SP800-90A DRBG State
    - Generation: SP800-90A DRBG State modification (instantiate, generate, etc.)
    - Establishment: N/A
    - Entry: N/A
    - Output: N/A
    - Storage: Plaintext in RAM
    - Key-to-Entity: Process
    - Zeroization: Power cycle and "fips zeroize all" command

12.4 Passwords & Related Secrets

14. User Password
    - Description: Password used to authenticate User (8 to 48 characters)
    - Type: Authentication data
    - Generation: N/A
    - Establishment: N/A
    - Entry: Configured by the operator, entered encrypted/authenticated over SSHv2 session
    - Output: MD5 hashed in configuration, output in plaintext (obfuscated) over RADIUS session, output encrypted/authenticated over SSHv2 session
    - Storage: MD5 digest in plaintext in Compact Flash
    - Key-to-Entity: User
    - Zeroization: "fips zeroize all" command

15. Port Administrator Password
    - Description: Password used to authenticate Port Configuration Administrator (8 to 48 characters)
    - Type: Authentication data
    - Generation: N/A
    - Establishment: N/A
    - Entry: Configured by the operator, entered encrypted/authenticated over SSHv2 session

- Output: MD5 hashed in configuration, output in plaintext (obfuscated) over RADIUS session, output encrypted/authenticated over SSHv2 session
- Storage: MD5 digest in plaintext in Compact Flash
- Key-to-Entity: User
- Zeroization: "fips zeroize all" command

16. Crypto Officer Password
    - Description: Password used to authenticate Crypto Officer (8 to 48 characters)
    - Type: Authentication data
    - Generation: N/A
    - Establishment: N/A
    - Entry: Configured by the operator, entered encrypted/authenticated over SSHv2 session
    - Output: MD5 hashed in configuration output in plaintext (obfuscated) over RADIUS session, output encrypted/authenticated over SSHv2 session
    - Storage: MD5 digest in plaintext in Compact Flash
    - Key-to-Entity: User
    - Zeroization: "fips zeroize all" command

17. RADIUS Secret
    - Description: Used to authenticate the RADIUS server (8 to 64 characters)
    - Type: Authentication data
    - Generation: N/A
    - Establishment: N/A
    - Entry: Configured by the operator, entered encrypted/authenticated over SSHv2 session
    - Output: MD5 hashed in configuration, MD5 hashed in RADIUS message, output encrypted/authenticated over SSHv2 session
    - Storage: Plaintext in RAM, proprietary two-way encrypted using base-64 (plaintext) in RAM and Compact Flash
    - Key-to-Entity: Process
    - Zeroization: "fips zeroize all" command

12.5 Miscellaneous

18. SNMPv3 secret
    - Description: Used for authentication (SHA1, Password is 8 to 16 characters long) and for privacy (AES-CFB 128-bit, Password 12 to 20 characters)
    - Type: Authentication data and privacy
    - Generation: N/A - generated outside of the module
    - Establishment: N/A
    - Entry: Configured by the operator, entered encrypted/authenticated over SSHv2 session
    - Output: SHA1 hashed in configuration, output encrypted / authenticated over SSHv2 session
    - Storage: SHA1 digest and AES are stored in Compact Flash
    - Key-to-Entity: Process: User
    - Zeroization: Session termination and "fips zeroize all" command

19. NTP secret
    - Description: Authentication (SHA1, Password is 8 to 16 characters long)
    - Type: Authentication data

- Generation: N/A - generated outside of the module
- Establishment: N/A
- Entry: Configured by the operator, entered authenticated over SSHv2 session
- Output: SHA1 hashed in configuration, output authenticated over SSHv2 session
- Storage: SHA1 digest is stored in Compact Flash
- Key-to-Entity: Process: User
- Zeroization: Session termination and "fips zeroize all" command

13 Public Keys

13.1 Firmware

1. Firmware Integrity / Firmware Load RSA Public Key
   - Description: RSA 2048-bit public key used to verify signature of firmware of the module
   - Type: RSA Public Key
   - Generation: N/A, Generated outside the module
   - Establishment: N/A
   - Entry: Through firmware update
   - Output: N/A
   - Storage: Plaintext in RAM, Plaintext in Compact Flash
   - Key-to-Entity: Process

13.2 SSHv2

2. SSHv2 Host RSA Public Key
   - Description: (2048 bit); Used to establish shared secrets
   - Type: RSA Public Key
   - Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method.
   - Establishment: N/A
   - Entry: Configured by the operator; Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
   - Output: Plaintext
   - Storage: Plaintext in RAM, Plaintext in Compact Flash
   - Key-to-Entity: Process

3. SSHv2 Client RSA Public Key
   - Description: (2048 bit); Used to establish shared secrets
   - Type: RSA Public Key
   - Generation: N/A, generated outside the module
   - Establishment: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
   - Entry: Configured by the operator; Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
   - Output: N/A
   - Storage: Plaintext in RAM, Plaintext in Compact Flash
   - Key-to-Entity: Process

4. SSHv2 DH Public Key
   - Description: (2048 bit modulus); Used to establish shared secrets (SSHv2 and DHCHAP)
   - Type: DH Public Key
   - Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the finite field is the output of the SP800-90A DRBG; allowed method as per FIPS 140-2 IG D.8 Scenario 4
   - Establishment: N/A
   - Entry: N/A

- Output: Plaintext
- Storage: Plaintext in RAM, Plaintext in Compact Flash
- Key-to-Entity: Process

5. SSHv2 DH Peer Public Key
   - Description: (2048 bit modulus); Used to establish shared secrets (SSHv2 and DHCHAP)
   - Type: DH Peer Public Key
   - Generation: N/A
   - Establishment: N/A
   - Entry: Plaintext
   - Output: N/A
   - Storage: Plaintext in RAM
   - Key-to-Entity: Process

13.3 TLS

6. TLS Client Public Key (RSA 2048 bit)
   - Description: Used to establish TLS session (passed to server)
   - Type: TLS Client Public key
   - Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method.
   - Establishment: N/A
   - Entry: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9 and SP800-38F §3.1
   - Output: Plaintext
   - Storage: Plaintext in RAM, Plaintext in Compact Flash
   - Key-to-Entity: Process

7. TLS Peer Public Key (RSA 2048 bit)
   - Description: Used to authenticate the server
   - Type: TLS Peer Public Key
   - Generation: N/A
   - Establishment: N/A
   - Entry: Plaintext during TLS v1.1 and v1.2 handshake protocol
   - Output: N/A
   - Storage: Plaintext in RAM, Plaintext in Compact Flash
   - Key-to-Entity: Process